

PRINTABLE GUIDE

Check a suspicious email before acting

Phishing messages seek money, information or harmful actions. Familiar logos and polished wording are easy to copy. No single visual check guarantees an email is genuine.

Any email app or website | 2 min read | 5 steps

Before you start

- ☐ A trusted contact route for the claimed sender
- ☐ The message left untouched while you check

1. Pause before interacting

Do not open attachments, follow links, scan an included QR code or reply with personal information. Pause at urgency, threats, unexpected refunds or requests for codes.

- ☐ Done this step

2. Inspect the request and sender

Look at the full email address and what the message wants you to do. A near-matching address, unexpected payment change or unusual request is suspicious. Correct spelling and a real-looking address do not prove authenticity.

- ☐ Done this step

3. Check through another route

Open the organisation's app yourself or type its known website address. Call a number from a statement or established contact record. For a friend's request, contact them separately rather than replying to the message you are checking.

☐ Done this step

4. Report and remove it

Use your mail service's Report phishing or Report spam control. In the UK, forward suspicious emails to report@phishing.gov.uk when appropriate, then delete them. Do not follow any reporting instruction contained in the suspicious message itself.

☐ Done this step

5. Act if you already responded

If you shared a password, change it through the genuine service from a trusted device. If financial information or money was involved, contact your bank promptly. Keep evidence and seek relevant support if you opened or installed something.

☐ Done this step

Try it for yourself

Keep a paper note of the trusted route you use to contact your bank.

☐ I tried the task.

My notes

Should I click Unsubscribe on suspicious mail?

Avoid interacting with a suspicious message. Use your mail service's reporting controls; unsubscribe only from genuine services you recognise.

Official help and the online guide

NCSC suspicious-email advice - <https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-email>

Recognise phishing in Outlook -

<https://support.microsoft.com/en-us/outlook/mail/phishing-and-suspicious-behavior-in-outlook>

Read online: <https://plaintechguides.com/guides/suspicious-email-checklist/>